Teaching Note:

**Ashley Madison Hacking: The Dark Web Gets Even Darker**

This teaching note was written by Koti Vinodbabu, under the direction of Debapratim Purkayastha, IBS Hyderabad.
Ashley Madison Hacking: The Dark Web Gets Even Darker

ABSTRACT

This case deals with the data hack issue involving the Ashley Madison website and emphasizes the importance of a secure management information and data security system for an organization. Ashley Madison, an infidelity website owned by Avid Living Media, was hacked by a group calling itself the Impact Team in July 2015. Impact stole the customer information profiles along with the sexual preferences and personal data of the users and threatened to shut down ALM’s network of cheating websites. They also threatened to publish the hacked data online if ALM did not shut down those websites. ALM did not take any step toward closure of the websites but assured its customers that their data was safe. Eventually, Impact put the data on different search engines like trustify.com. This created panic among the customers of Ashley Madison as they feared that exposure of their information online would destroy their existing relationships and their reputation.

TEACHING OBJECTIVES AND TARGET AUDIENCE

The case is designed to enable a student to:

1. Understand the issues and challenges involved in maintaining a secure management information system.
2. Analyze how Avid Life Media can cope with the data breach issue.
3. Explore ways to establish a network of reliable and safe online transactions.

This case is meant for MBA/MS students as a part of their Information Technology and Knowledge Management System curriculum. This can also be discussed as part of a Business Ethics curriculum.

TEACHING APPROACH AND STRATEGY

The discussion on the case can be taken further with the help of the following questions.

1. Critically analyze the data breach problem at Ashley Madison.
2. Discuss the aspects of a secure management information and data security system of an organization.
3. What are the precautionary strategies to be adopted to prevent a data hack?
1) **Critically analyze the data breach problem at Ashley Madison.**

The Ashley Madison website offered its members the opportunity to have a “discreet” extramarital relationship by providing them with a platform to contact other like-minded members. The site was run based on paid memberships. While subscribing to the site, users had to provide their details and sexual preferences and the website assured them that these were confidential. However, the Impact Team stole the data from Ashley Madison and alleged that the website was destroying relationships by giving members a chance to cheat on their partners. It was unethical for anyone who was in a relationship to cheat on their partners in society but Ashley Madison encouraged such activity by giving them options to go in for a discreet relationship with others, it said. The Impact Team did not appear to be interested in financial gain or to have a political agenda. Instead, its motivation was moral outrage. Any organization can face moral outrage irrespective of whether it has happy customers or not. This kind of outrage might lead to the shutdown of the organization too. So, the motivations of hackers are changing with the emergence of ‘hacktivists’, who pursue sensitive data for alternative ends.

Apart from its morally questionable business model, Ashley Madison did not have a secure management information system. This can be gauged from the fact that the Impact Team could so easily gain access to confidential data from the website. By agreeing to install apps on a device, a customer is said to be willing to share his/her data with third parties. But he/she does not know where exactly the data goes. Sometimes it can have uncomfortable implications like in the case of Ashley Madison where the hackers stole sensitive customer information and threatened to expose the identities of its 37 million users. Sensitive information of the customers including names, email addresses, and credit card information were dumped online for all to see. In addition to the company losing credibility in the eyes of its customers, the data breach led to ominous implications for some including the embarrassment of being exposed, ruined marriages, and suicides in some extreme cases.

Having a secure information storage system is essential for any organization as the breach of confidential information by third parties may lead to the total collapse of the organization. In most cases this data is protected by layers of security, encryption, policy, and regulation, but that is not always effective as was seen in the Ashley Madison case. Beyond data security, the aspect to be observed is how this data is actually used by the businesses. It is important for a company to ascertain which data is worthy of security measures more rigorous than the minimum required. While Ashley Madison considered passwords and credit card numbers (stored only the last four digits) sensitive enough to warrant additional protection, considering the nature of its business it should also have provided similar attention to user names, contact information, and highly sensitive comments on what they were expecting from an affair partner. However, even the passwords were not found to be safe as Ashley Madison’s protect-in-place strategy for its password data using data hashes was found wanting.

Ashley Madison also failed to deliver on its key customer value proposition of providing them with “discreet” affairs. It made promises to its users and the broader internet community that it failed to honor, and this hurt its reputation and made it vulnerable to lawsuits. It was very clear that despite offering an extra security feature to its members for an additional fee of US$19, the company did not completely erase the user’s profile and all data associated with the user.

The problem in dealing with ‘hacktivists’ is that it becomes essential for companies to undertake preventive measures despite not knowing their identities and motives. But it is surprising to see that Ashley Madison did not learn a lesson from the data hacking episode involving the Adult FriendFinder website to safeguard the data of its subscribers.
For an organization, effective crisis management is crucial in data breach situations. Ashley Madison released a statement assuring its members that it would take care of the data breach situation. Within 24 hours of the breach, it assured customers that it had closed any security holes that had allowed the data breach to occur. But subsequent investigation by experts showed that this was not the case. Preventive security measures against future attacks are essential for Ashley Madison at this crucial time.

2) Discuss the aspects of security and control in the information system of an organization.

Security and control in the information system of an organization involves actions to prevent illegal access, modification, or deletion of information. The reasons for the data breach may be

1. Unintentional threats which involve
   - Human error – in the design or use of the system
   - Environmental hazards – acts of God and others
   - Computer system failures – faulty products

2. Intentional threats

   Systems are subject to a wide variety of hazards from criminal attacks.

   It is not possible to secure the data system unless the organization understands the risks involved in data security. The possible risks for the organizational data are listed here.

1) Risk to Software

   a) Hacking

      Hacking is the unauthorized access and use of networked computer systems. Ashley Madison’s data was hacked by Impact.
      - It is the unauthorized use, access, modification, and destruction of hardware, software, data, or network resources.
      - It is the unauthorized release of information
      - It is the unauthorized copying of software
      - It denies an end user access to his or her own hardware, software, data, or network resources
      - Illegal hackers (also called crackers) frequently attack the internet and other networks to steal or damage data and programs.
      - Hackers can monitor e-mail, web server access, or file transfers to extract passwords or steal network files, or to plant data that will cause a system to allow intruders to access the systems
      - Hackers use remote services that allow one computer on a network to execute programs on another computer to gain private access within a network.

   b) Cyber-Theft

      Many computer crimes involve the theft of money. They involve unauthorized network entry and fraudulent alternation of computer databases to cover the tracks of the employees involved.

   c) Unauthorized Use at Work

      This may range from doing private consulting or personal finances, or playing video games to unauthorized use of the internet on company networks.
d) Software Piracy
Unauthorized copying of software or software piracy is a major form of software theft because software is intellectual property, protected by copyright law and user licensing agreements.

e) Piracy of Intellectual Property
Software is not the only intellectual property subject to computer-based piracy. Other forms of copyrighted material, such as music, videos, images, articles, books, and other written works are also considered as intellectual property.

f) Computer Viruses and Worms
A virus is a program code that cannot work without being inserted into another program. A worm is a distinct program that can run unaided. Viruses and worms typically enter a computer system through illegal or borrowed copies of software or through network links to other computer systems.

2) Risk to Hardware
a) Natural Disasters
• Disasters that pose a risk include fires, floods, and hurricanes, which can destroy hardware and software and can causing total or partial paralysis of systems and communications lines.

b) Blackout & Brownout
• Blackout – losses due to high electrical power.
• Brownout – the voltage of power decreases at short interruptions in the flow of power.
• Vandalism – occurs when human beings deliberately destroy computer systems.

3) What are the precautionary strategies to be adopted to prevent a data hack?
Companies must protect all sensitive information like the personal information of customers and employees, intellectual property secrets, passwords, and private keys using secure system settings. The time at which a data security breach occurs is not the right time to develop a data security plan. Implementing a proactive approach is a better plan and it shows the stakeholders that the organization had made an attempt to secure the data. The responsibility of data security lies not only with the owners of the business and IT professionals but with all the members of the organization. Creating a culture of data security in the organization is important. Certain defence strategies against data hacking are listed here. Ashley Madison should have used these strategies to protect its data.

1. Encryption
• Passwords, messages, files, and other data can be transmitted in scrambled form and unscrambled by computer systems for authorized users only.
• Encryption involves using special mathematical algorithms, or keys, to transform digital data into a scrambled code before they are transmitted, and to decode the data when they are received.

2. Authentication
• Authentication is a critical part of a security system. It is part of the process referred to as Identification and Authentication (I&A). The identification process starts when a user ID or Login name is typed into a sign-on screen. Authentication methods are based on one or more of three factors. 1) Password or PIN. 2) Smart card or an identification device. 3) Fingerprints or retinal pattern.
3. **Firewalls**

- Firewall software is another important method for control and security on the internet and other networks. A network firewall can be a communications processor, a router, or a dedicated server, along with firewall software.
- A firewall serves as a gatekeeper for the computer system.
- A firewall computer screens all network traffic for proper passwords and other security.
- A firewall only allows authorized transmissions in and out of the network.
- Firewalls have become an essential component of organizations connecting to the internet.
- Firewalls can check, but not completely prevent unauthorized access (hacking) into computer networks.

4. **E-Mail Monitoring**

Internet and other online e-mail systems are one of the preferred ways of attack by hackers for spreading computer viruses or breaking into networked computers.

5. **Virus Defences (Antivirus Software)**

An antivirus software scans the computer’s memory, disks, and all the email. It uses a virus definition file that is updated regularly.

6. **Backup Files**

Backup files, which are duplicate files of data or programs, are another important security measure. Files can be protected by file retention measures that involve storing copies of files from previous periods.

7. **Security Monitors**

System security monitors are software programs that monitor the use of computer systems and networks and protect them from unauthorized use, fraud, and destruction.

8. **Biometric Controls**

They use physical characteristics to identify the user like voice verification, fingerprints, signature dynamics and retina scanning, face recognition, and genetic pattern analysis.

The following are some of the measures for data security and secure management information systems.

- Protect the office or data center with alarms and monitoring systems.
- Enforce restrictions on internet access.
- Keep computers and associated components out of public view.
- Ensure that the operating system is up to date.
- Fight off hacking attacks with intrusion detection technology.
- Ensure that the anti-malware solution is up to date.
- Utilize a protected power supply and backup energy sources.

With big companies like Sony being rendered vulnerable, it goes a long way to show that companies have not taken cyber security as seriously as they should. Small and Medium Enterprises should be especially vigilant as these businesses often lack IT support to keep an eye out for potential cyber threats, making them easy targets. With sensitive
information like credit card details, passwords, and personal information at stake, it is high time everyone gave cyber security the attention it deserves. A data breach could potentially threaten the survival of an SME as it may not have the resources to recover from it. Companies should zealously do the following:

**Conduct cyber risk assessments –**
- Identify and pre-empt the risks that the company – employees, processes, and technology – is exposed to.
- Conduct individualized risk assessment to identify its most sensitive data.
- The accuracy of a risk assessment is critical.
- Base information security management decisions on accurate cyber risk assessments.
- Risk assessments also enable investments on controls to be balanced against the business harm likely to result from security failures.

**Educate and train employees** -
- Insider crimes can prove to be more costly or damaging.
- Invest in security awareness training for employees on information security best practice as well as cyber threats.
- Such initiatives also help meet specific compliance requirements mandated by ISO 27001 and the PCI DSS.

**Evaluate cyber risks from supply chain**
- Hackers can enter a company’s networks through its suppliers, or even the suppliers’ suppliers.
- Supply chain partners should be scrutinized and it should be ensured that they comply with their privacy and security policies.

**Test the organization’s networks**
- Regular penetration tests should be conducted in order to identify exploitable security loopholes and vulnerabilities in hardware and software, and remedial action should be taken.
- A systematic approach (such as ISO 27001) should be adopted to manage sensitive company information so that it remains secure by applying a risk management process that includes people, processes, and IT systems.

**Create a triage-based system for protecting information** – An organization cannot take every conceivable measure to protect every piece of data; risk mitigation must be balanced with cost and efficiency of business processes.
Suggested Readings and References:

15. Rob Price, “The strange rise and sudden fall of Noel Biderman, the former CEO of Ashley Madison,” www.businessinsider.in, August 28, 2015.


38. www.ksl.com/?nid=151&sid=35580017